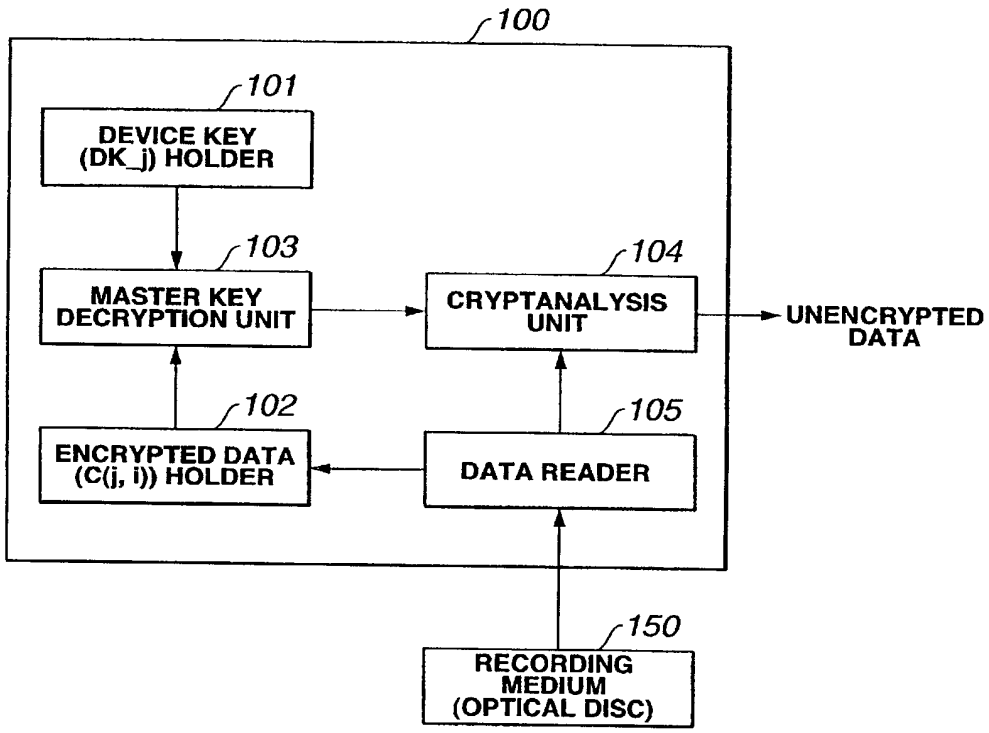
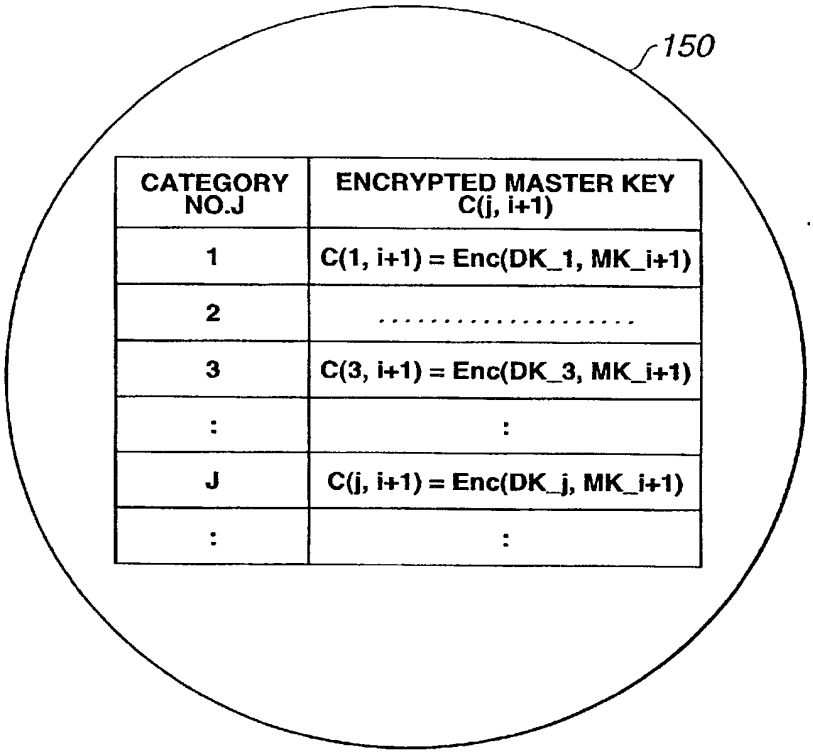

100
101
DEVICE KEY (DK_j) HOLDER
103
MASTER KEY DECRYPTION UNIT
104
CRYPTANALYSIS UNIT
UNENCRYPTED DATA
102
ENCRYPTED DATA (C(j, i)) HOLDER
105
DATA READER
150
RECORDING MEDIUM (OPTICAL DISC)

FIG.1



CATEGORY NO.J	ENCRYPTED MASTER KEY C(j, i+1)
1	C(1, i+1) = Enc(DK_1, MK_i+1)
2	.....
3	C(3, i+1) = Enc(DK_3, MK_i+1)
:	:
J	C(j, i+1) = Enc(DK_j, MK_i+1)
:	:

FIG.2

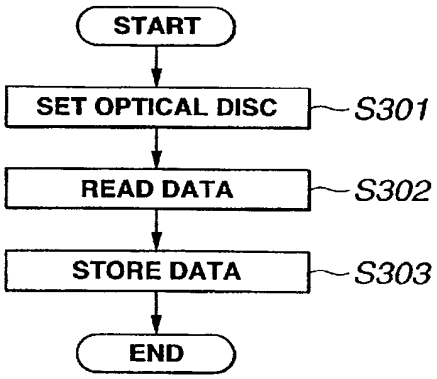


FIG.3

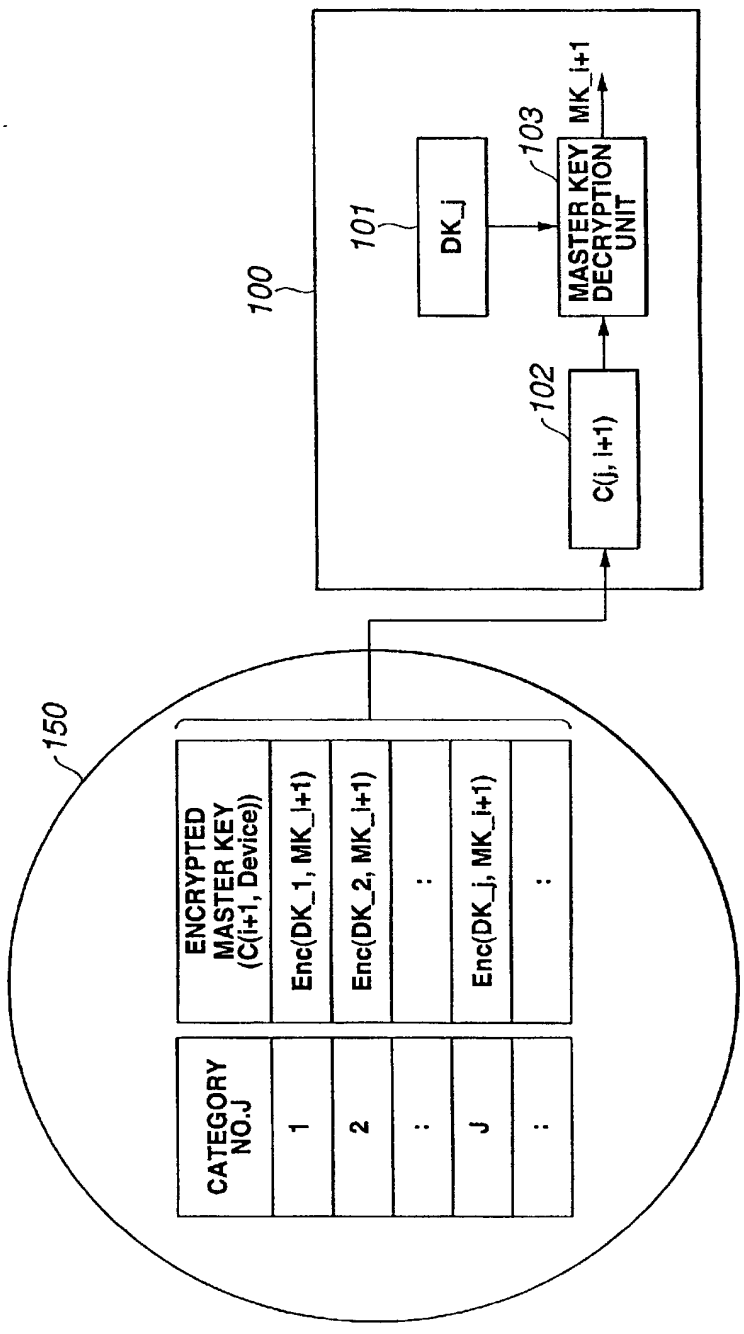

150
CATEGORY NO.J
ENCRYPTED MASTER KEY (C(i+1, Device))
1
Enc(DK_1, MK_i+1)
2
Enc(DK_2, MK_i+1)
J
Enc(DK_j, MK_i+1)
100
101
DK_j
102
C(j, i+1)
103
MASTER KEY DECRYPTION UNIT
MK_i+1

FIG.4

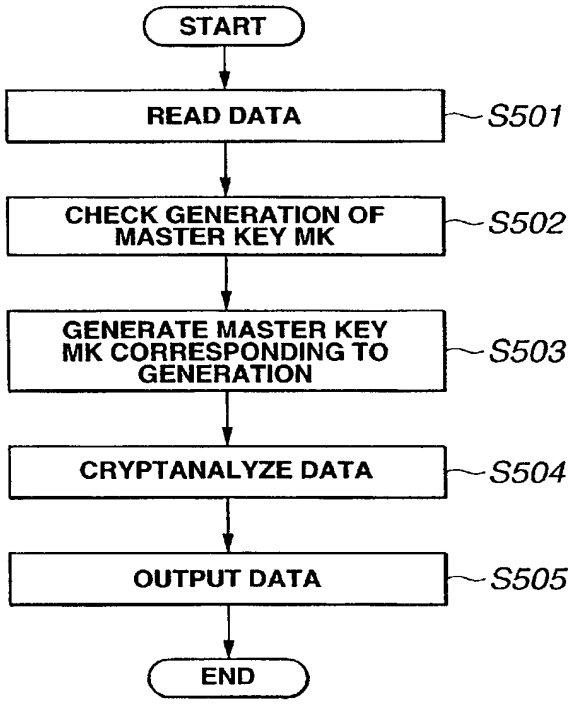

START
READ DATA
S501
CHECK GENERATION OF MASTER KEY MK
S502
GENERATE MASTER KEY MK CORRESPONDING TO GENERATION
S503
CRYPTANALYZE DATA
S504
OUTPUT DATA
S505
END

FIG.5

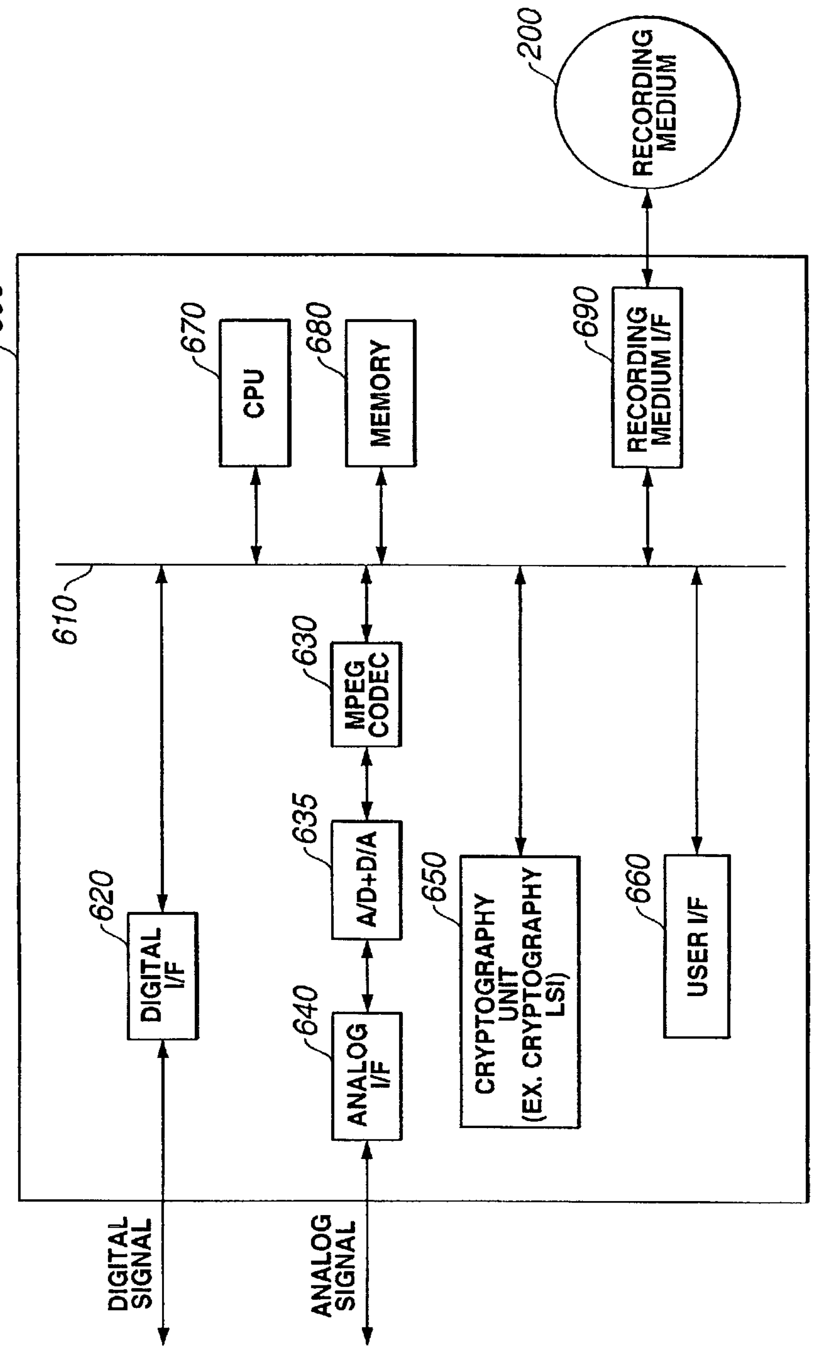


FIG.6

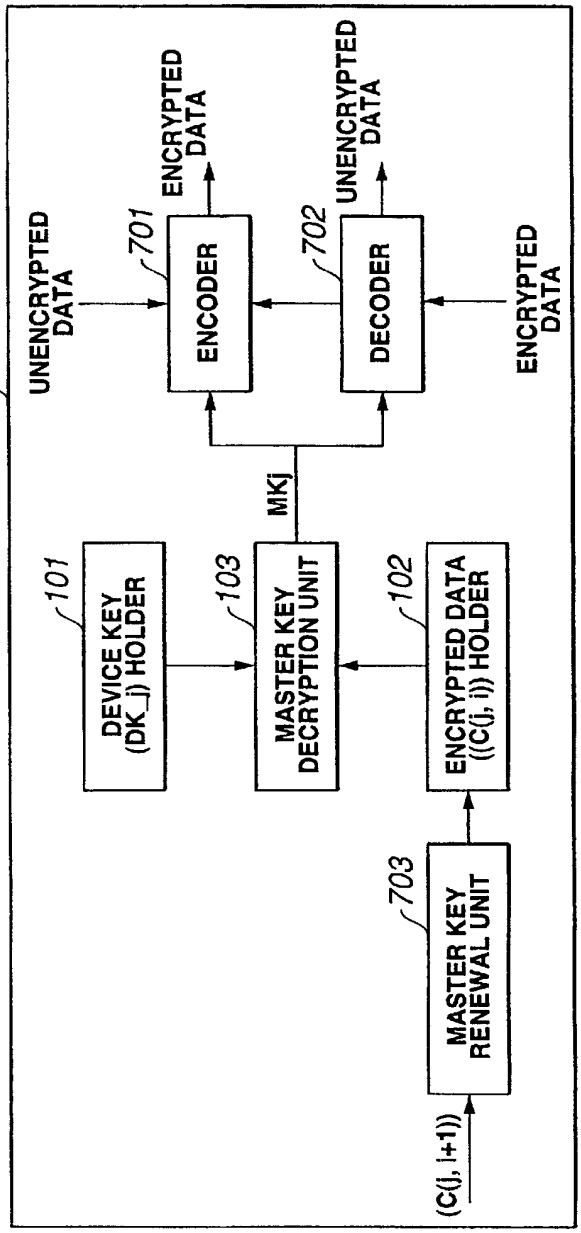

650
UNENCRYPTED DATA
701
ENCODER
ENCRYPTED DATA
702
DECODER
UNENCRYPTED DATA
ENCRYPTED DATA
MKj
101
DEVICE KEY (DK_j) HOLDER
103
MASTER KEY DECRYPTION UNIT
102
ENCRYPTED DATA ((C(j, i)) HOLDER
703
MASTER KEY RENEWAL UNIT
(C(j, i+1))

FIG.7

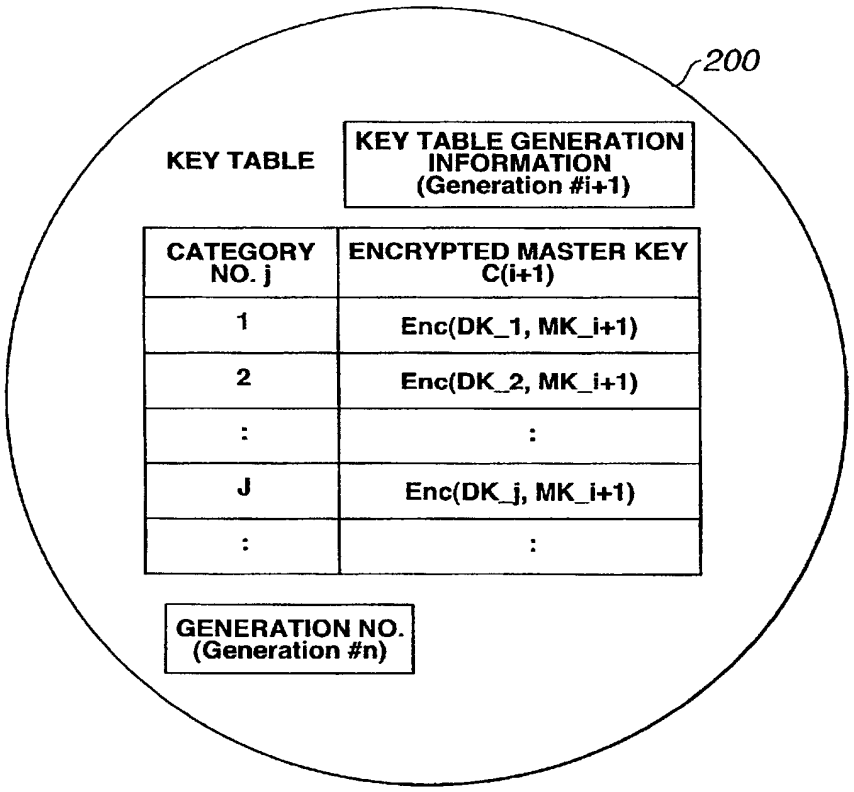

200
KEY TABLE
KEY TABLE GENERATION INFORMATION (Generation #i+1)
CATEGORY NO. j
ENCRYPTED MASTER KEY C(i+1)
1
Enc(DK_1, MK_i+1)
2
Enc(DK_2, MK_i+1)
:
:
J
Enc(DK_j, MK_i+1)
:
:
GENERATION NO. (Generation #n)

FIG.8

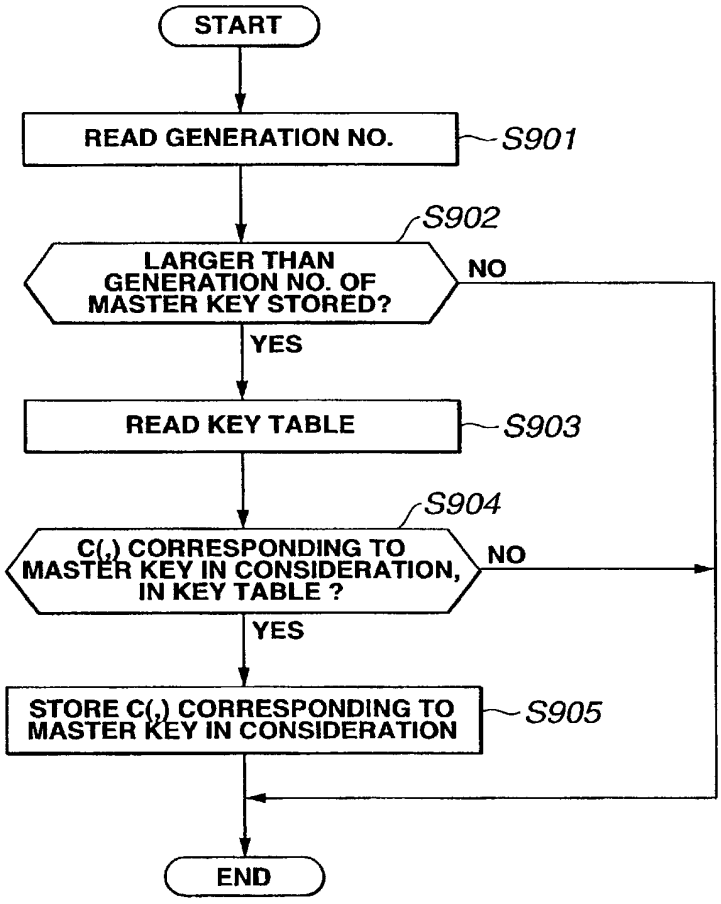

START
READ GENERATION NO.
S901
S902
LARGER THAN GENERATION NO. OF MASTER KEY STORED?
NO
YES
READ KEY TABLE
S903
S904
C(,) CORRESPONDING TO MASTER KEY IN CONSIDERATION, IN KEY TABLE ?
NO
YES
STORE C(,) CORRESPONDING TO MASTER KEY IN CONSIDERATION
S905
END

FIG.9

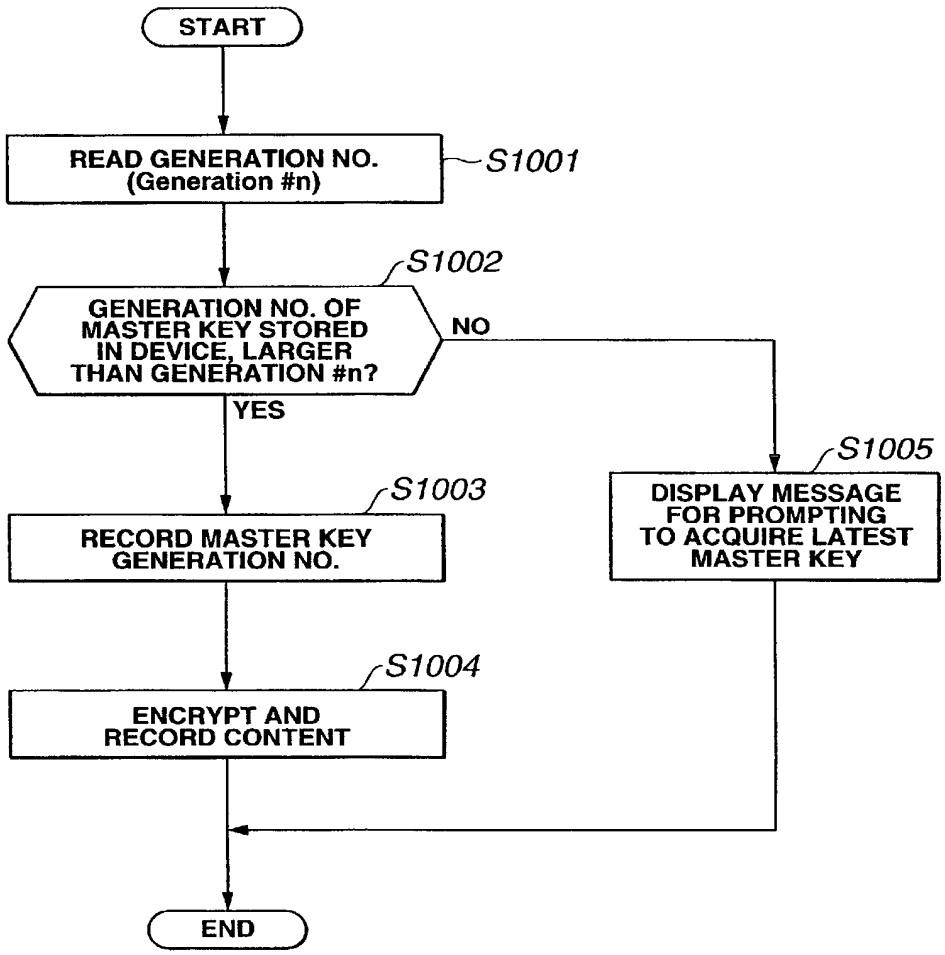

START
READ GENERATION NO. (Generation #n)
S1001
S1002
GENERATION NO. OF MASTER KEY STORED IN DEVICE, LARGER THAN GENERATION #n?
NO
YES
S1003
RECORD MASTER KEY GENERATION NO.
S1004
ENCRYPT AND RECORD CONTENT
S1005
DISPLAY MESSAGE FOR PROMPTING TO ACQUIRE LATEST MASTER KEY
END

FIG.10

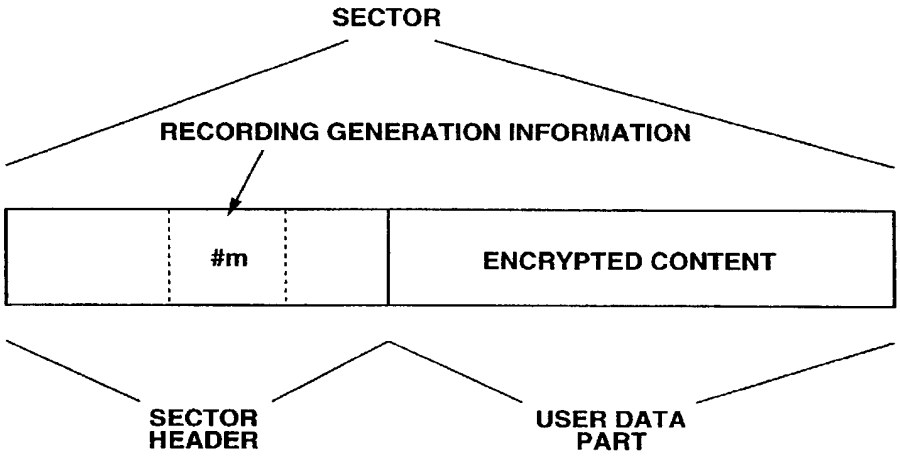

SECTOR
RECORDING GENERATION INFORMATION
#m
ENCRYPTED CONTENT
SECTOR HEADER
USER DATA PART

FIG.11

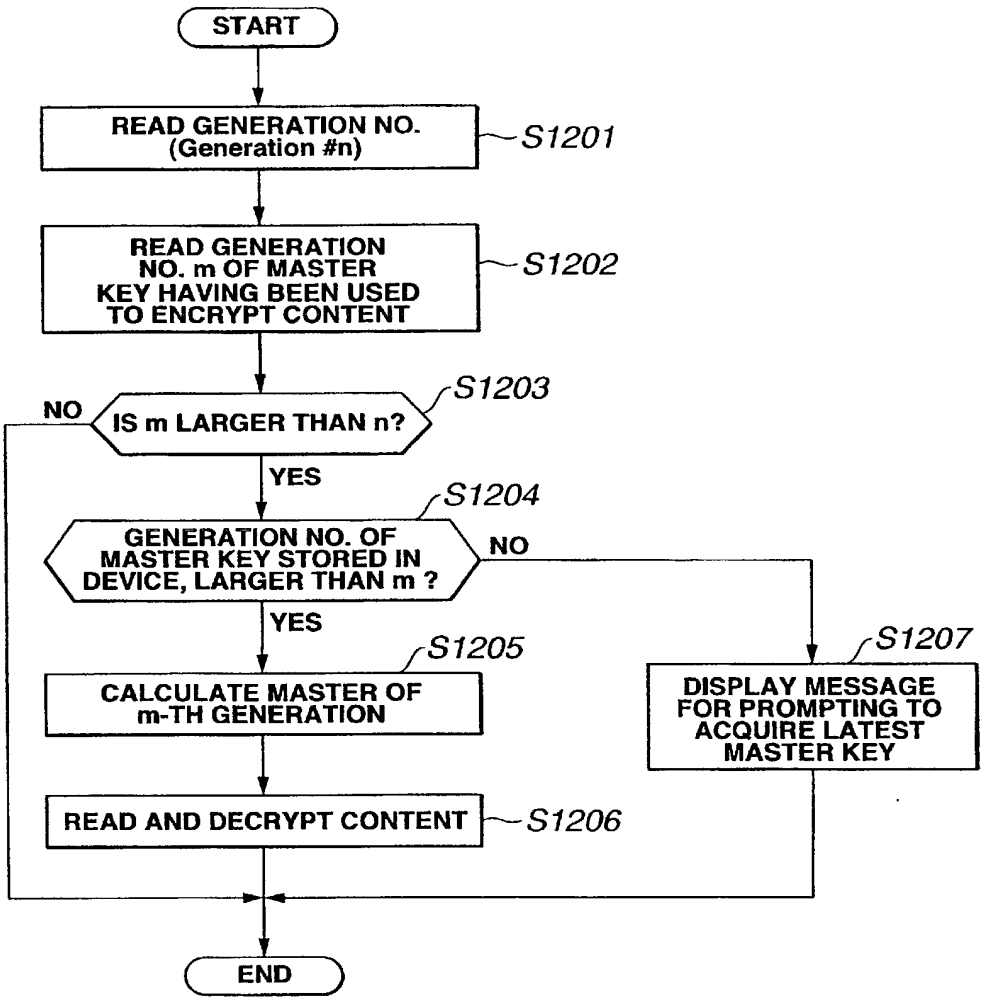

START
READ GENERATION NO. (Generation #n)
S1201
READ GENERATION NO. m OF MASTER KEY HAVING BEEN USED TO ENCRYPT CONTENT
S1202
IS m LARGER THAN n?
S1203
NO
YES
GENERATION NO. OF MASTER KEY STORED IN DEVICE, LARGER THAN m ?
S1204
NO
YES
CALCULATE MASTER OF m-TH GENERATION
S1205
DISPLAY MESSAGE FOR PROMPTING TO ACQUIRE LATEST MASTER KEY
S1207
READ AND DECRYPT CONTENT
S1206
END

FIG.12

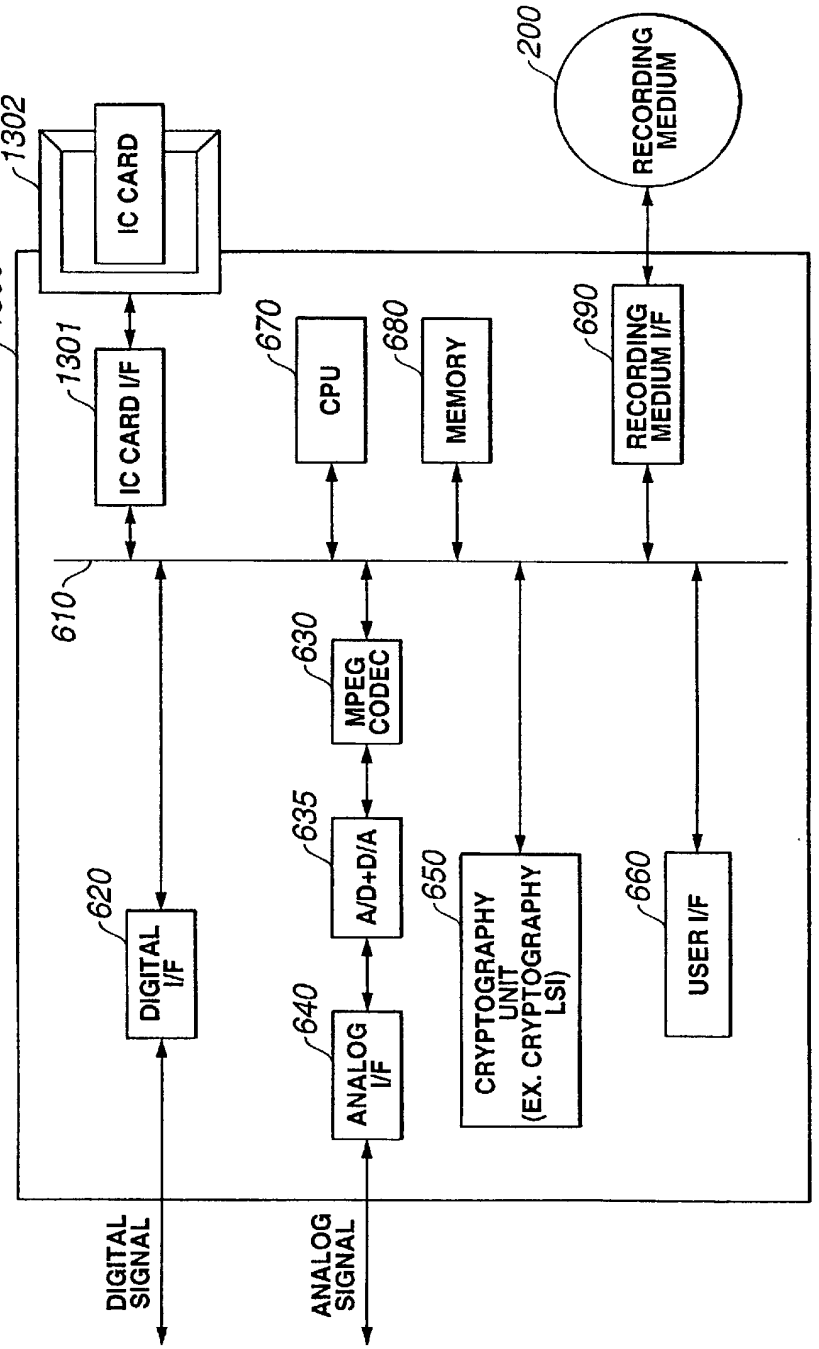

200
RECORDING MEDIUM
1302
IC CARD
1300
1301
IC CARD I/F
670
CPU
680
MEMORY
690
RECORDING MEDIUM I/F
610
630
MPEG CODEC
635
A/D+D/A
640
ANALOG I/F
620
DIGITAL I/F
650
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
660
USER I/F
DIGITAL SIGNAL
ANALOG SIGNAL

FIG.13

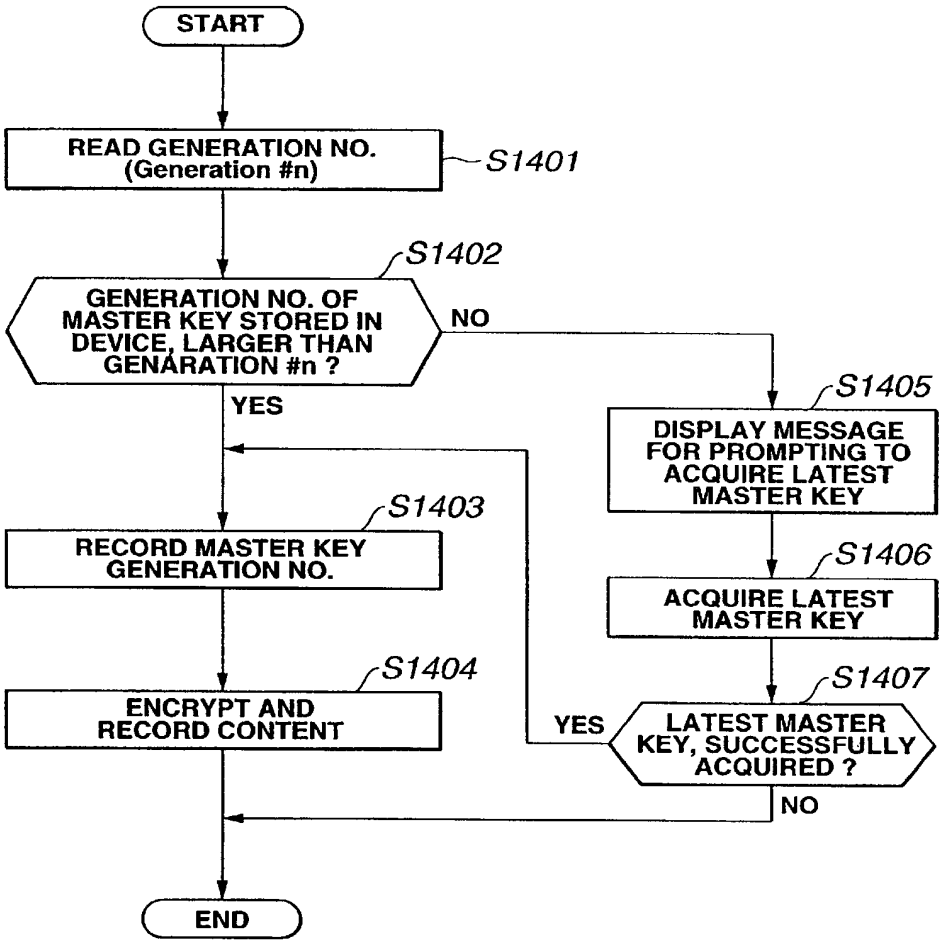

START
READ GENERATION NO. (Generation #n)
S1401
S1402
GENERATION NO. OF MASTER KEY STORED IN DEVICE, LARGER THAN GENARATION #n ?
NO
YES
S1405
DISPLAY MESSAGE FOR PROMPTING TO ACQUIRE LATEST MASTER KEY
S1403
RECORD MASTER KEY GENERATION NO.
S1406
ACQUIRE LATEST MASTER KEY
S1404
ENCRYPT AND RECORD CONTENT
S1407
YES
LATEST MASTER KEY, SUCCESSFULLY ACQUIRED ?
NO
END

FIG.14

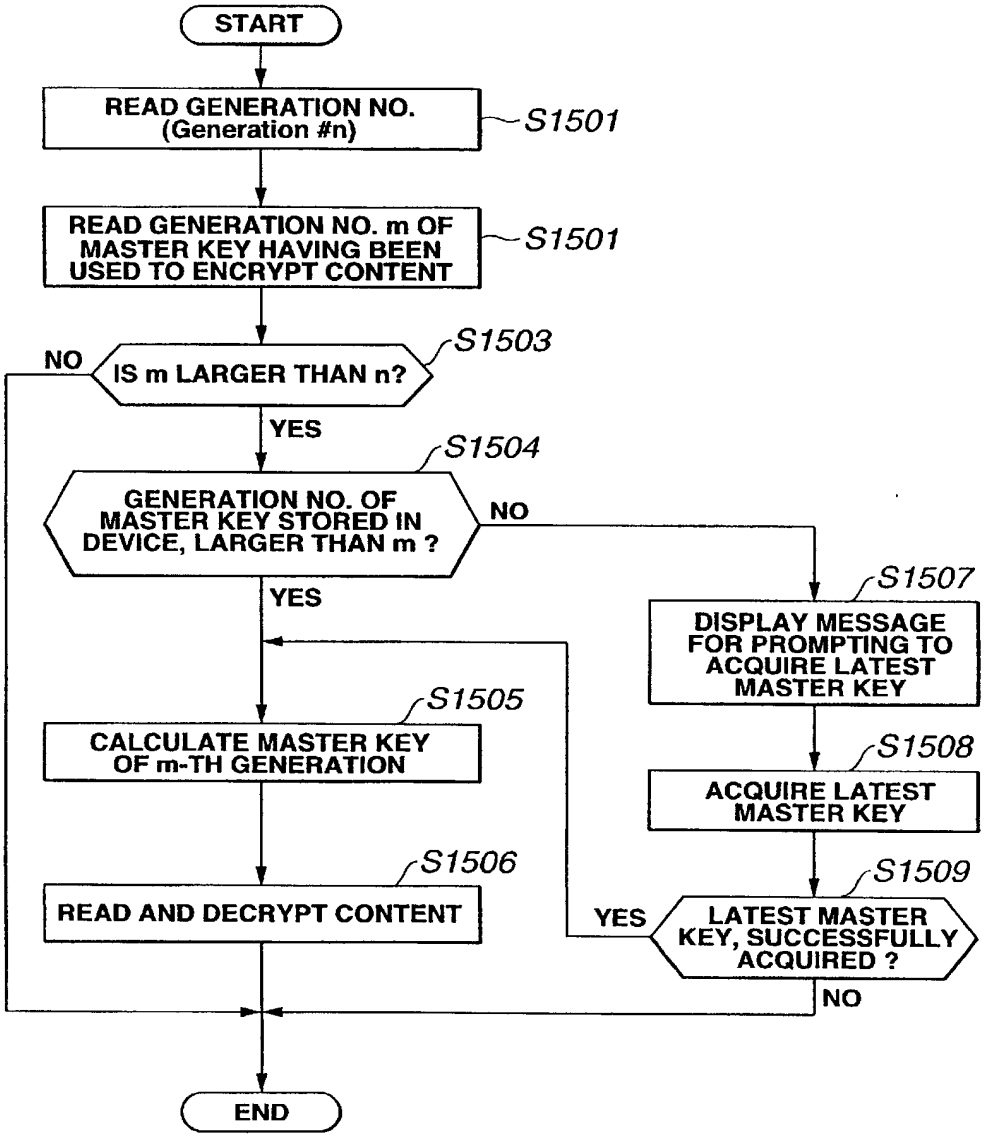

START
READ GENERATION NO. (Generation #n)
S1501
READ GENERATION NO. m OF MASTER KEY HAVING BEEN USED TO ENCRYPT CONTENT
S1501
S1503
NO
IS m LARGER THAN n?
YES
S1504
GENERATION NO. OF MASTER KEY STORED IN DEVICE, LARGER THAN m ?
NO
YES
S1507
DISPLAY MESSAGE FOR PROMPTING TO ACQUIRE LATEST MASTER KEY
S1505
CALCULATE MASTER KEY OF m-TH GENERATION
S1508
ACQUIRE LATEST MASTER KEY
S1506
READ AND DECRYPT CONTENT
S1509
YES
LATEST MASTER KEY, SUCCESSFULLY ACQUIRED ?
NO
END

FIG.15

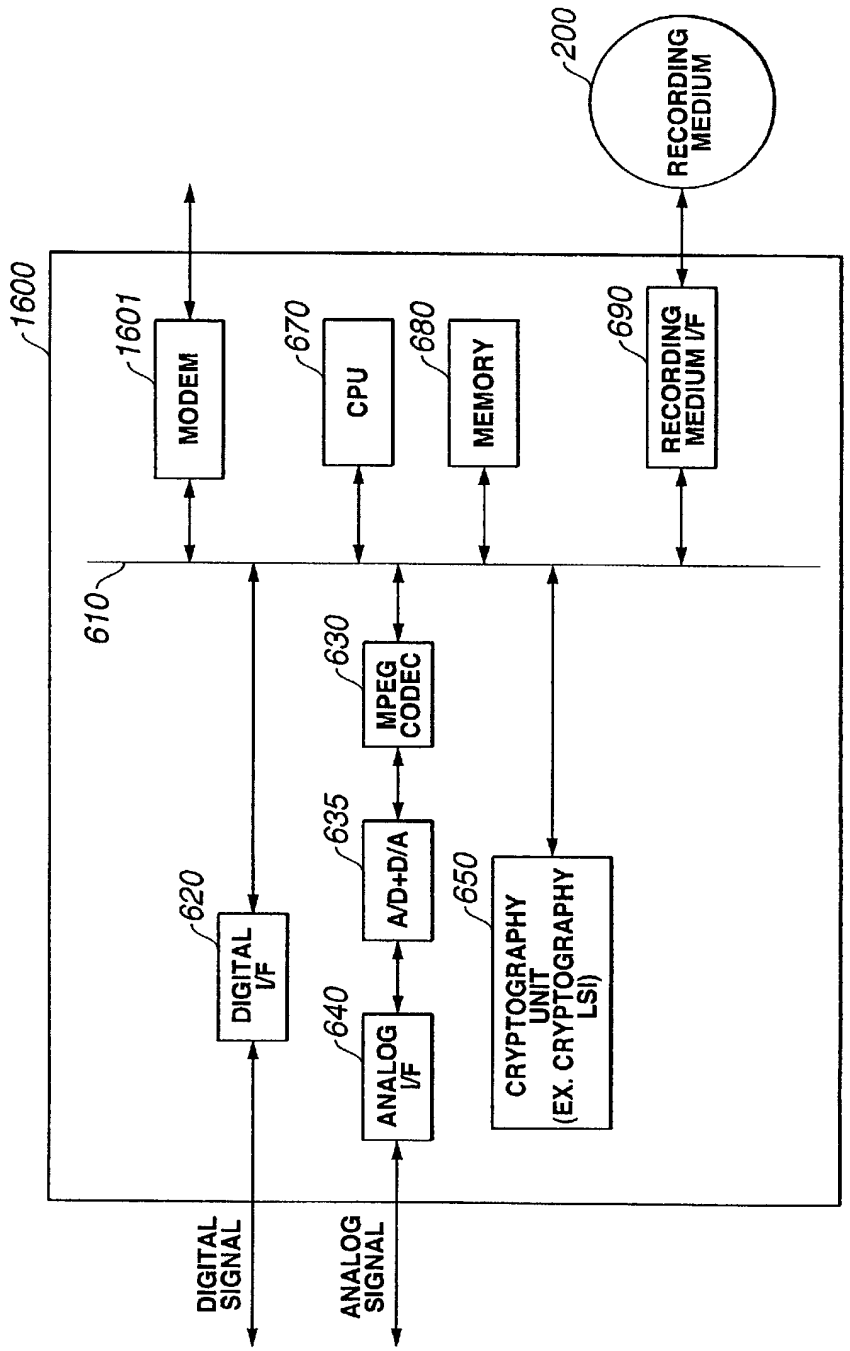

200
RECORDING MEDIUM
1600
1601
MODEM
670
CPU
680
MEMORY
690
RECORDING MEDIUM I/F
610
630
MPEG CODEC
635
A/D+D/A
620
DIGITAL I/F
640
ANALOG I/F
650
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
DIGITAL SIGNAL
ANALOG SIGNAL

FIG.16

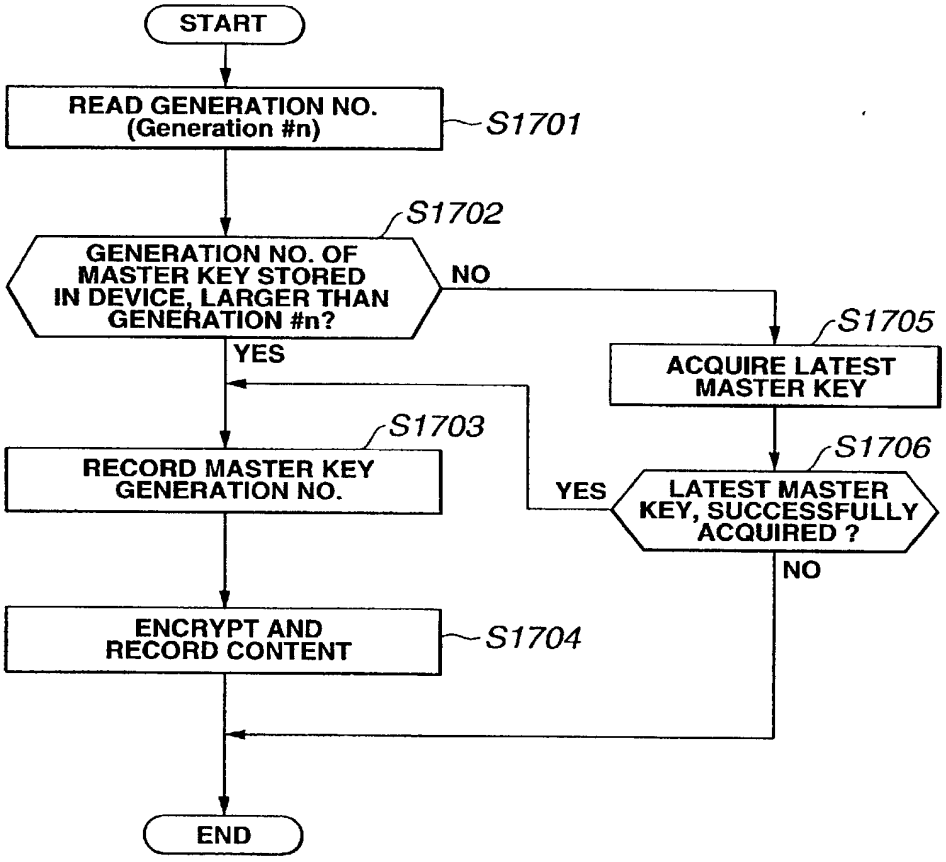

START
READ GENERATION NO. (Generation #n)
S1701
S1702
GENERATION NO. OF MASTER KEY STORED IN DEVICE, LARGER THAN GENERATION #n?
NO
YES
S1705
ACQUIRE LATEST MASTER KEY
S1703
RECORD MASTER KEY GENERATION NO.
S1706
YES
LATEST MASTER KEY, SUCCESSFULLY ACQUIRED ?
NO
ENCRYPT AND RECORD CONTENT
S1704
END

FIG.17

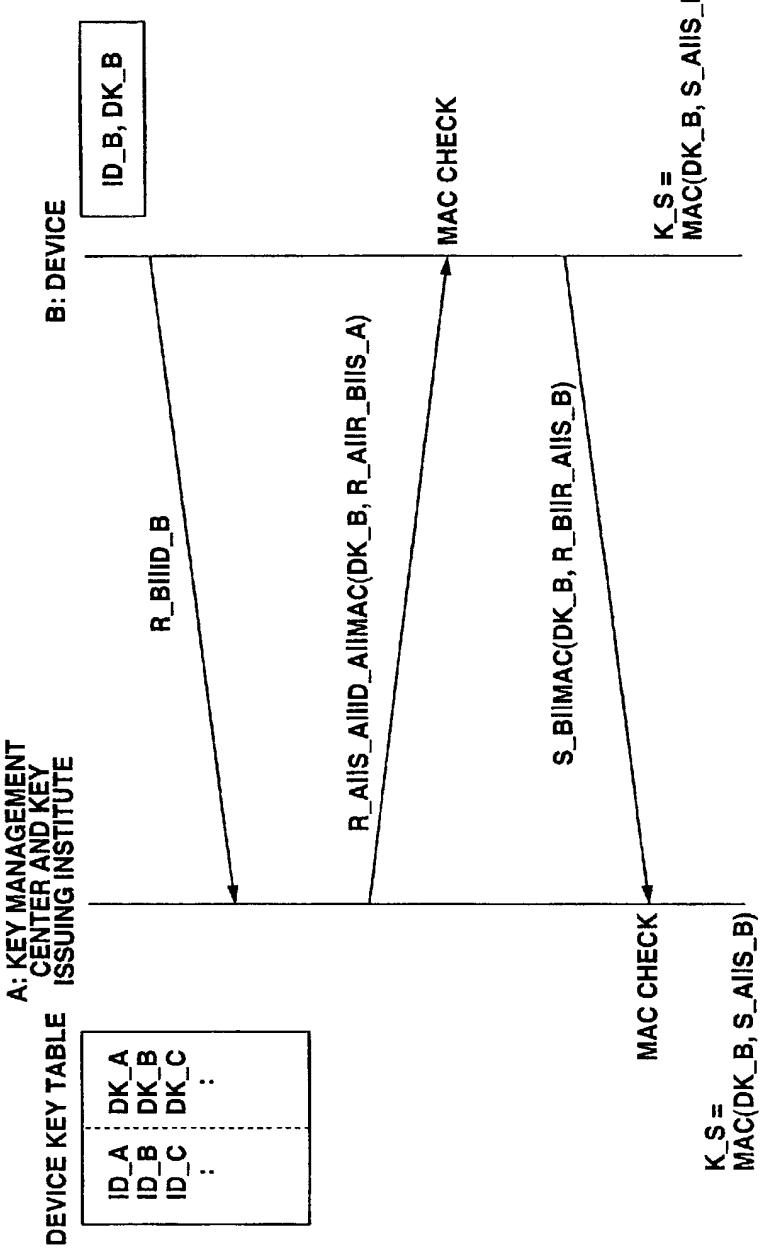

A: KEY MANAGEMENT CENTER AND KEY ISSUING INSTITUTE
DEVICE KEY TABLE
ID_A DK_A
ID_B DK_B
ID_C DK_C
B: DEVICE
ID_B, DK_B
R_BIIID_B
R_AIIS_AIIID_AIIMAC(DK_B, R_AIIR_BIIS_A)
S_BIIMAC(DK_B, R_BIIR_AIIS_B)
MAC CHECK
K_S = MAC(DK_B, S_AIIS_B)
MAC CHECK
K_S = MAC(DK_B, S_AIIS_B)

FIG.18

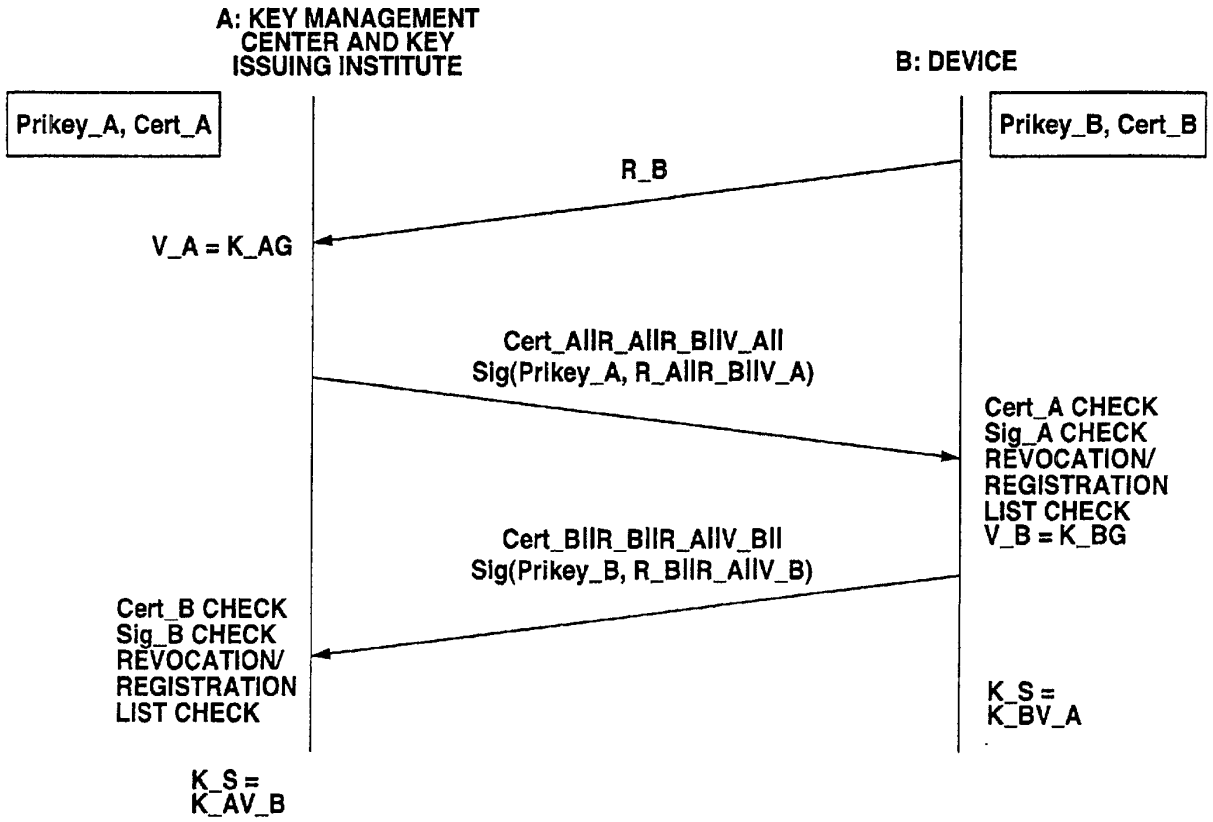

A: KEY MANAGEMENT CENTER AND KEY ISSUING INSTITUTE
B: DEVICE
Prikey_A, Cert_A
Prikey_B, Cert_B
R_B
V_A = K_AG
Cert_AIIR_AIIR_BIIV_AII
Sig(Prikey_A, R_AIIR_BIIV_A)
Cert_A CHECK
Sig_A CHECK
REVOCATION/
REGISTRATION
LIST CHECK
V_B = K_BG
Cert_BIIR_BIIR_AIIV_BII
Sig(Prikey_B, R_BIIR_AIIV_B)
Cert_B CHECK
Sig_B CHECK
REVOCATION/
REGISTRATION
LIST CHECK
K_S =
K_BV_A
K_S =
K_AV_B

FIG.19

ID OF B (ID_B)
PUBLIC KEY OF B (Pubkey_B)
DIGITAL SIGNATURE BY CENTER TO ALL ABOVE FIELDS

FIG.20

VERSION NO.
ID FOR DEVICE TO BE REVOKED
:
DIGITAL SIGNATURE BY CENTER

FIG.21

VERSION NO.
ID OF DEVICE TO BE REGISTERED
:
DIGITAL SIGNATURE BY CENTER

FIG.22

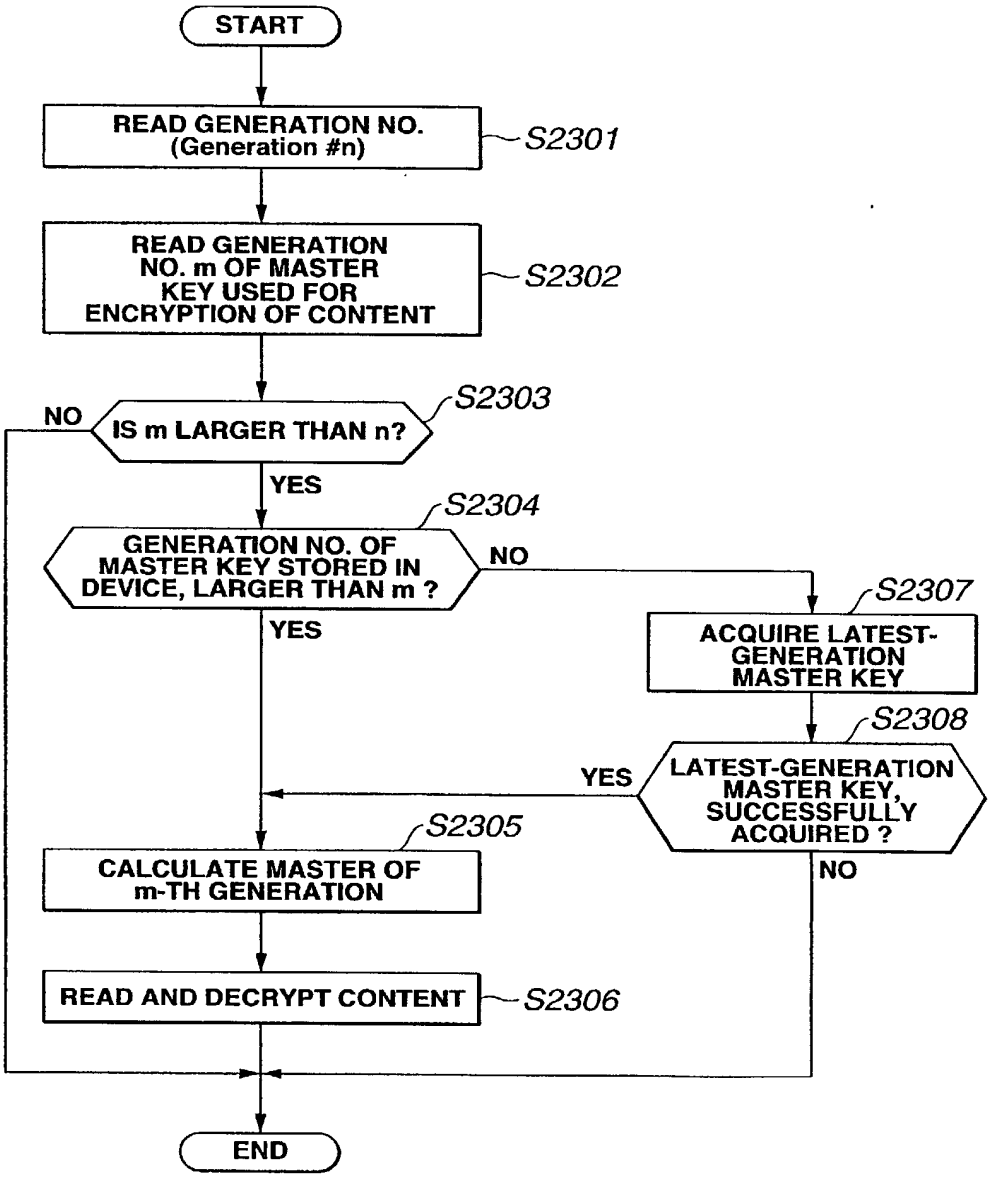

START
READ GENERATION NO. (Generation #n)
S2301
READ GENERATION NO. m OF MASTER KEY USED FOR ENCRYPTION OF CONTENT
S2302
NO
IS m LARGER THAN n?
S2303
YES
S2304
GENERATION NO. OF MASTER KEY STORED IN DEVICE, LARGER THAN m ?
NO
YES
S2307
ACQUIRE LATEST-GENERATION MASTER KEY
S2308
YES
LATEST-GENERATION MASTER KEY, SUCCESSFULLY ACQUIRED ?
NO
S2305
CALCULATE MASTER OF m-TH GENERATION
READ AND DECRYPT CONTENT
S2306
END

FIG.23

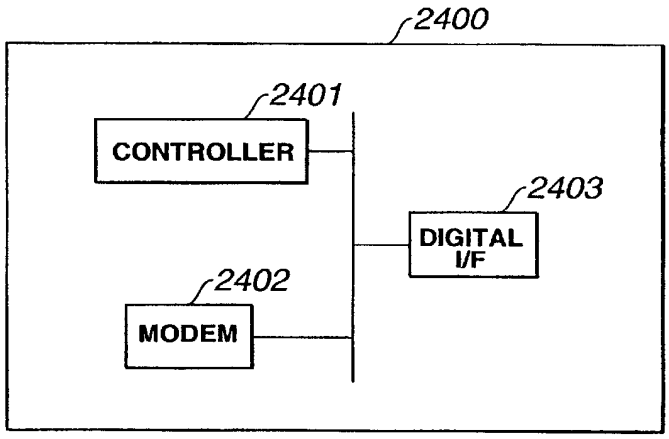


FIG.24

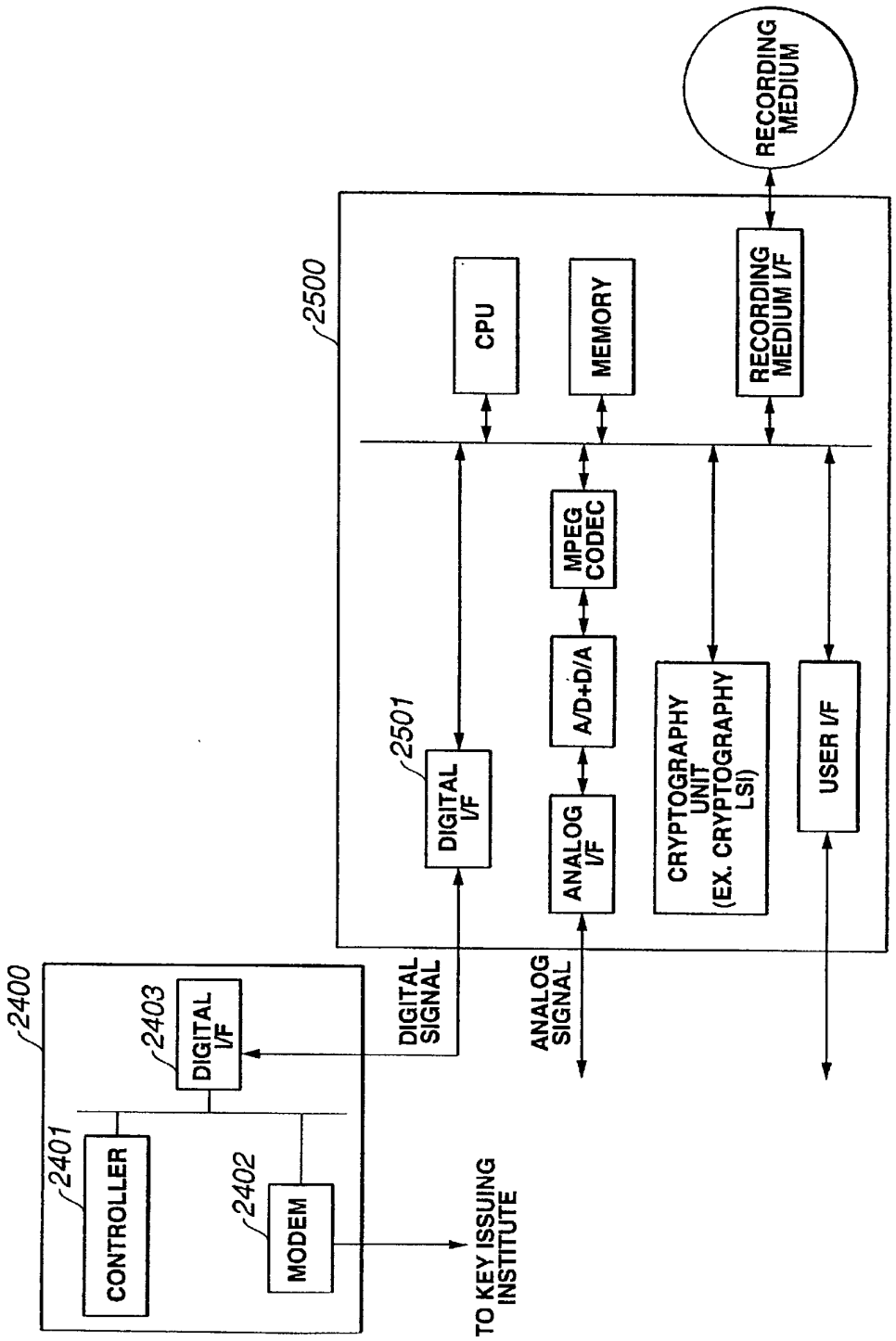

2400
2401
CONTROLLER
2402
MODEM
2403
DIGITAL I/F
TO KEY ISSUING INSTITUTE
DIGITAL SIGNAL
ANALOG SIGNAL
2500
2501
DIGITAL I/F
ANALOG I/F
A/D+D/A
MPEG CODEC
CPU
MEMORY
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
USER I/F
RECORDING MEDIUM I/F
RECORDING MEDIUM

FIG.25

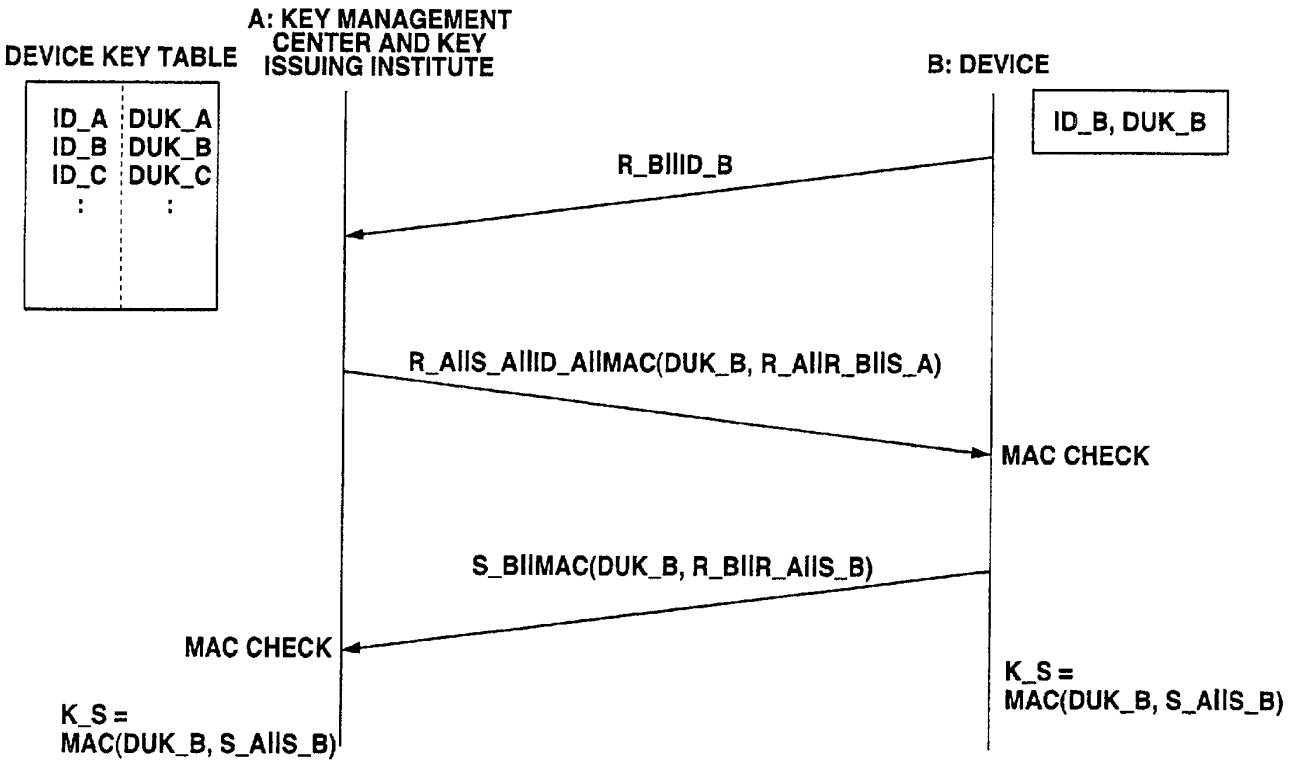

A: KEY MANAGEMENT CENTER AND KEY ISSUING INSTITUTE
DEVICE KEY TABLE
ID_A DUK_A
ID_B DUK_B
ID_C DUK_C
B: DEVICE
ID_B, DUK_B
R_BIIID_B
R_AIIS_AIIID_AIIMAC(DUK_B, R_AIIR_BIIS_A)
MAC CHECK
S_BIIMAC(DUK_B, R_BIIR_AIIS_B)
MAC CHECK
K_S = MAC(DUK_B, S_AIIS_B)
K_S = MAC(DUK_B, S_AIIS_B)

FIG.26

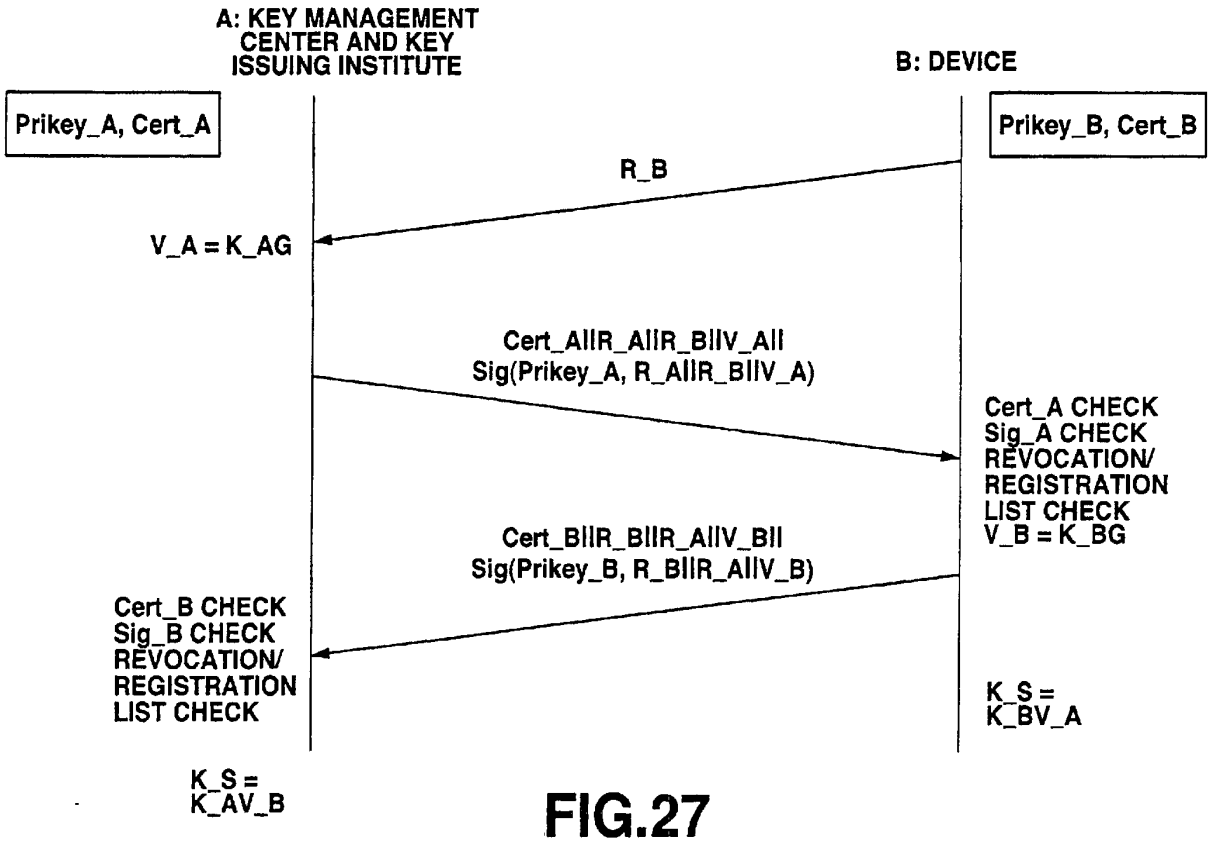

A: KEY MANAGEMENT CENTER AND KEY ISSUING INSTITUTE
B: DEVICE
Prikey_A, Cert_A
Prikey_B, Cert_B
R_B
V_A = K_AG
Cert_A||R_A||R_B||V_A||
Sig(Prikey_A, R_A||R_B||V_A)
Cert_A CHECK
Sig_A CHECK
REVOCATION/
REGISTRATION
LIST CHECK
V_B = K_BG
Cert_B||R_B||R_A||V_B||
Sig(Prikey_B, R_B||R_A||V_B)
Cert_B CHECK
Sig_B CHECK
REVOCATION/
REGISTRATION
LIST CHECK
K_S =
K_BV_A
K_S =
K_AV_B

FIG.27

GENERATION #n	
DEVICE UNIQUE IDENTIFICATION NUMBER (DEVICE ID)	ENCRYPTED MASTER KEY
1	Enc(DUK_1, MK_n)
2	Enc(DUK_2, MK_n)
:	:
L	Enc(DUK_L, MK_n)

FIG.28

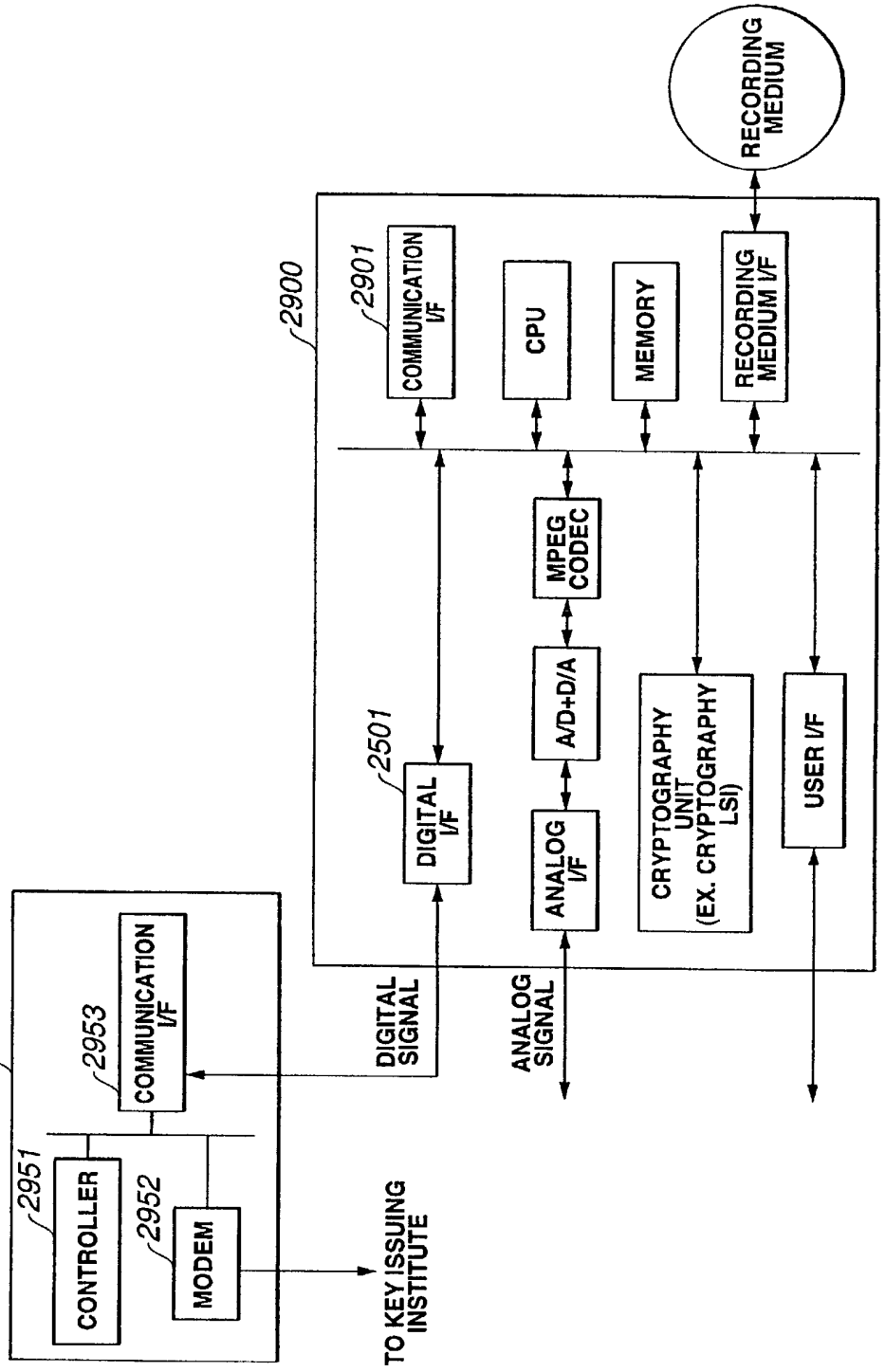

RECORDING MEDIUM
2900
2901
COMMUNICATION I/F
CPU
MEMORY
RECORDING MEDIUM I/F
MPEG CODEC
2501
DIGITAL I/F
A/D+D/A
ANALOG I/F
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
USER I/F
DIGITAL SIGNAL
ANALOG SIGNAL
2950
2953
COMMUNICATION I/F
2951
CONTROLLER
2952
MODEM
TO KEY ISSUING INSTITUTE

FIG.29

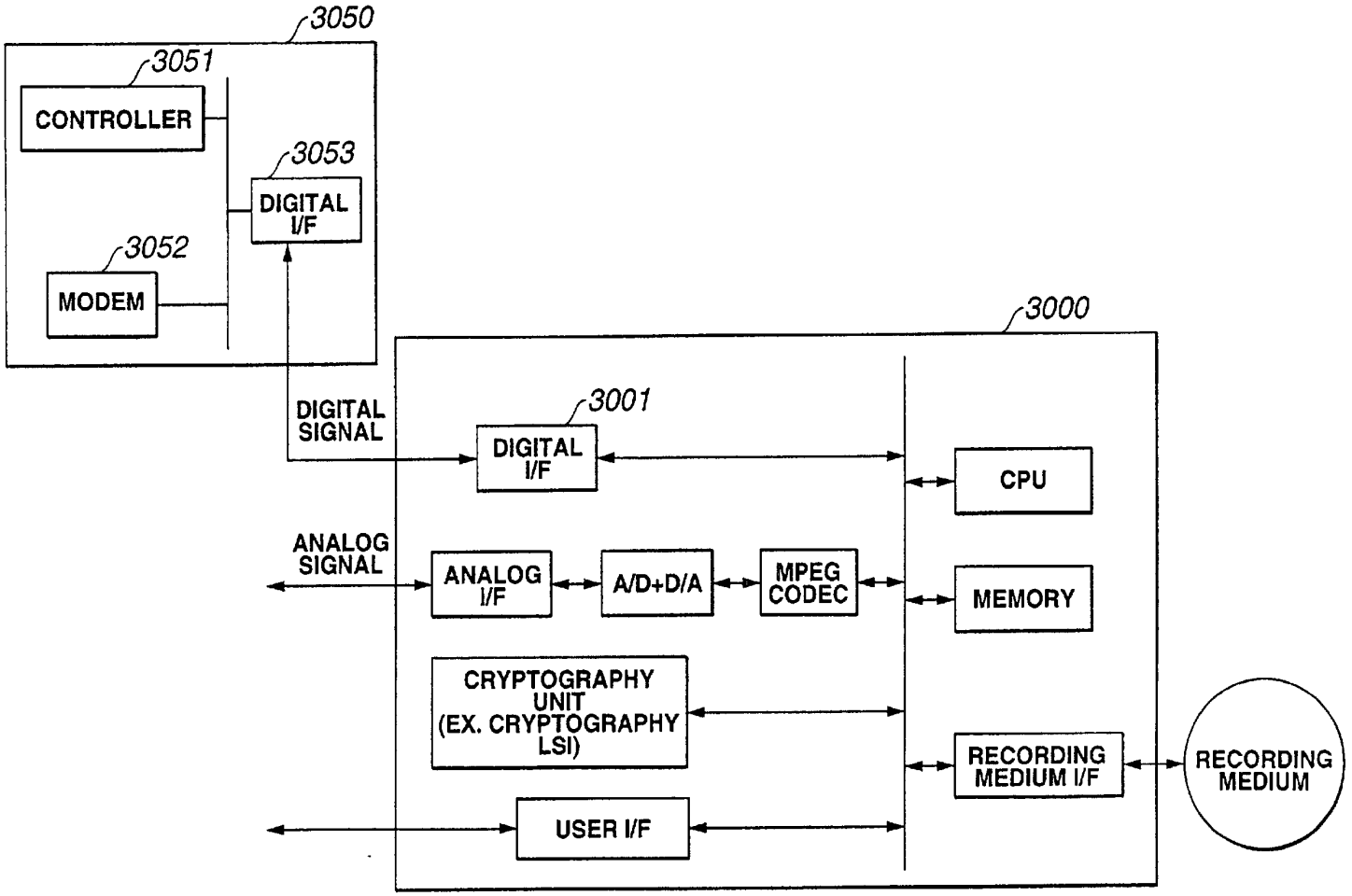

3050
3051
CONTROLLER
3053
DIGITAL I/F
3052
MODEM
3000
DIGITAL SIGNAL
3001
DIGITAL I/F
CPU
ANALOG SIGNAL
ANALOG I/F
A/D+D/A
MPEG CODEC
MEMORY
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
RECORDING MEDIUM I/F
RECORDING MEDIUM
USER I/F

FIG.30

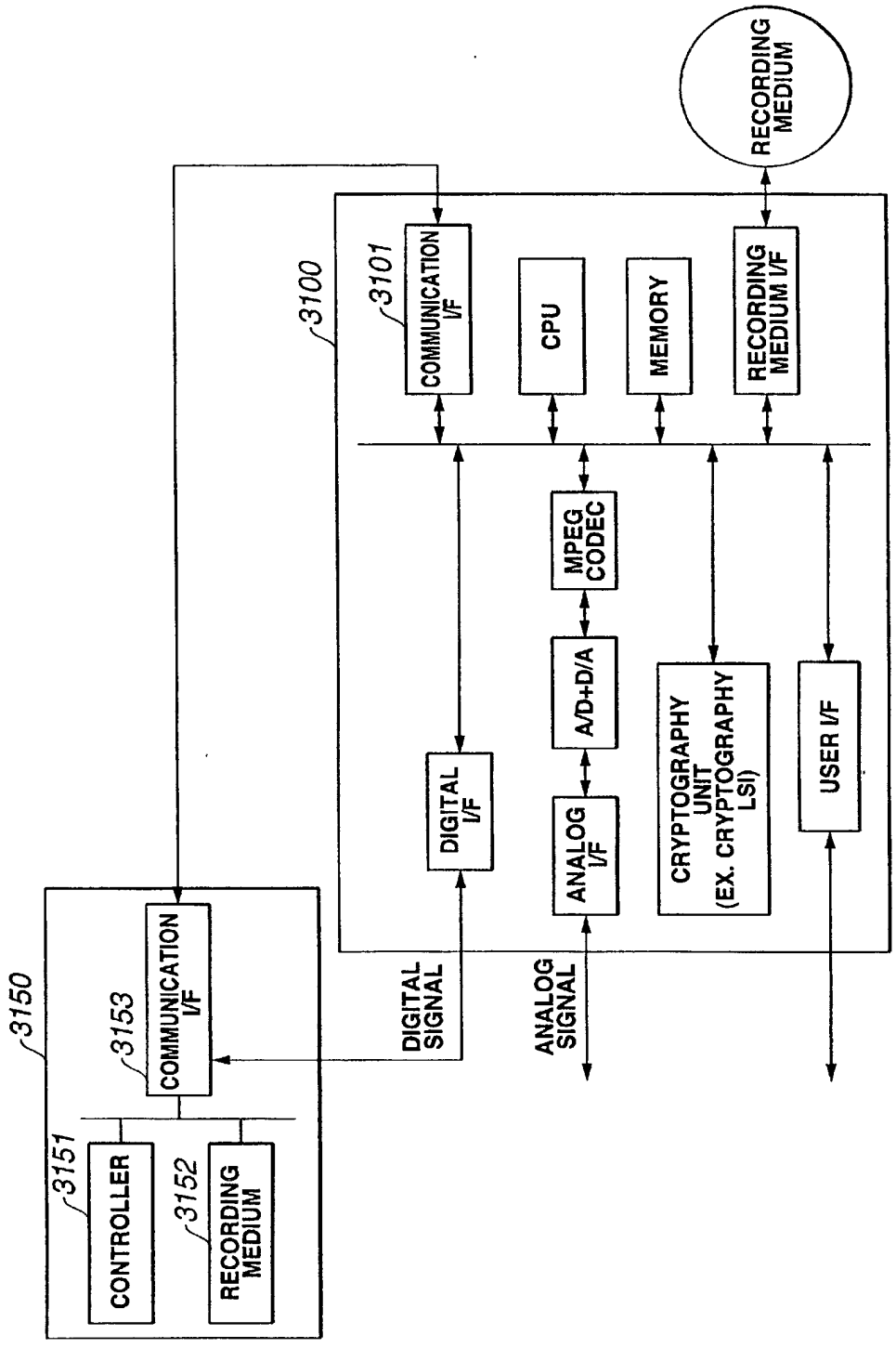

RECORDING MEDIUM
3100
3101
COMMUNICATION I/F
CPU
MEMORY
RECORDING MEDIUM I/F
MPEG CODEC
A/D+D/A
ANALOG I/F
DIGITAL I/F
CRYPTOGRAPHY UNIT (EX. CRYPTOGRAPHY LSI)
USER I/F
DIGITAL SIGNAL
ANALOG SIGNAL
3150
3153
COMMUNICATION I/F
3151
CONTROLLER
3152
RECORDING MEDIUM

FIG.31

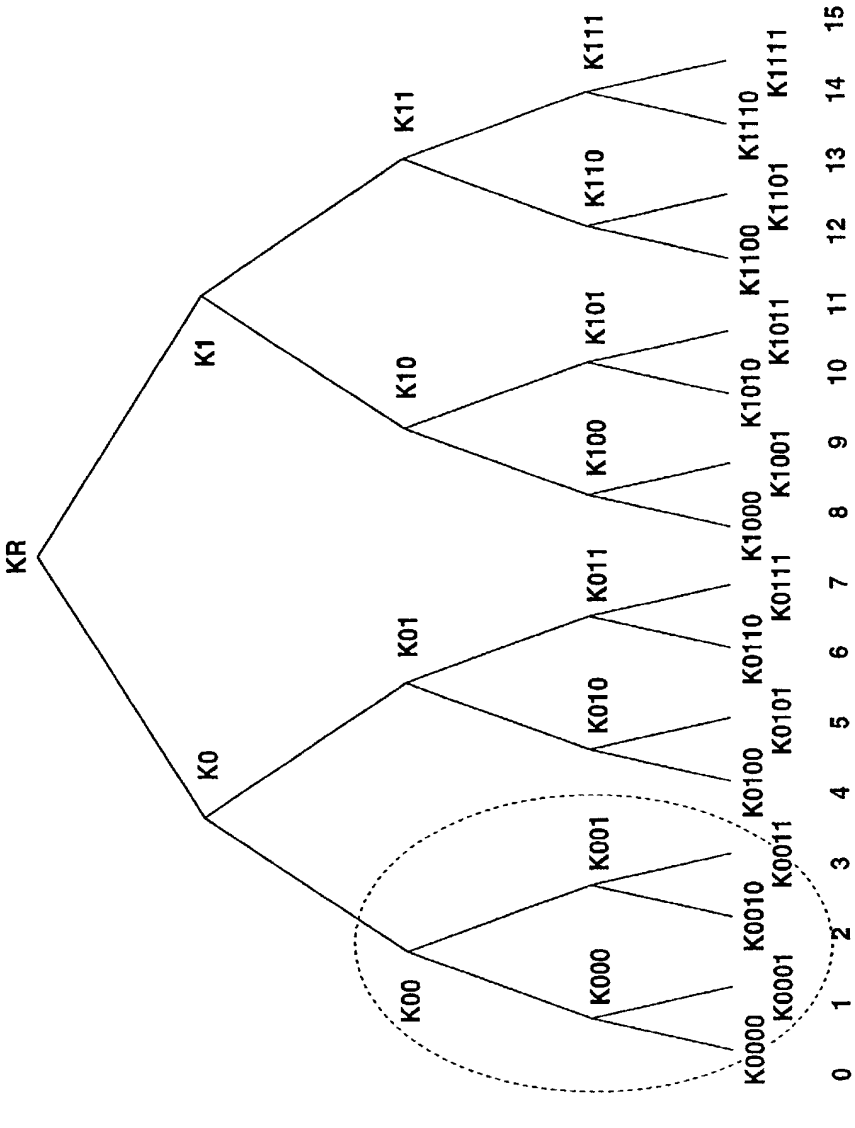

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
DEVICE

FIG.32

GENERATION : t	
INDEX	ENCRYPTION KEY
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.33A

GENERATION : t	
INDEX	ENCRYPTION KEY
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.33B

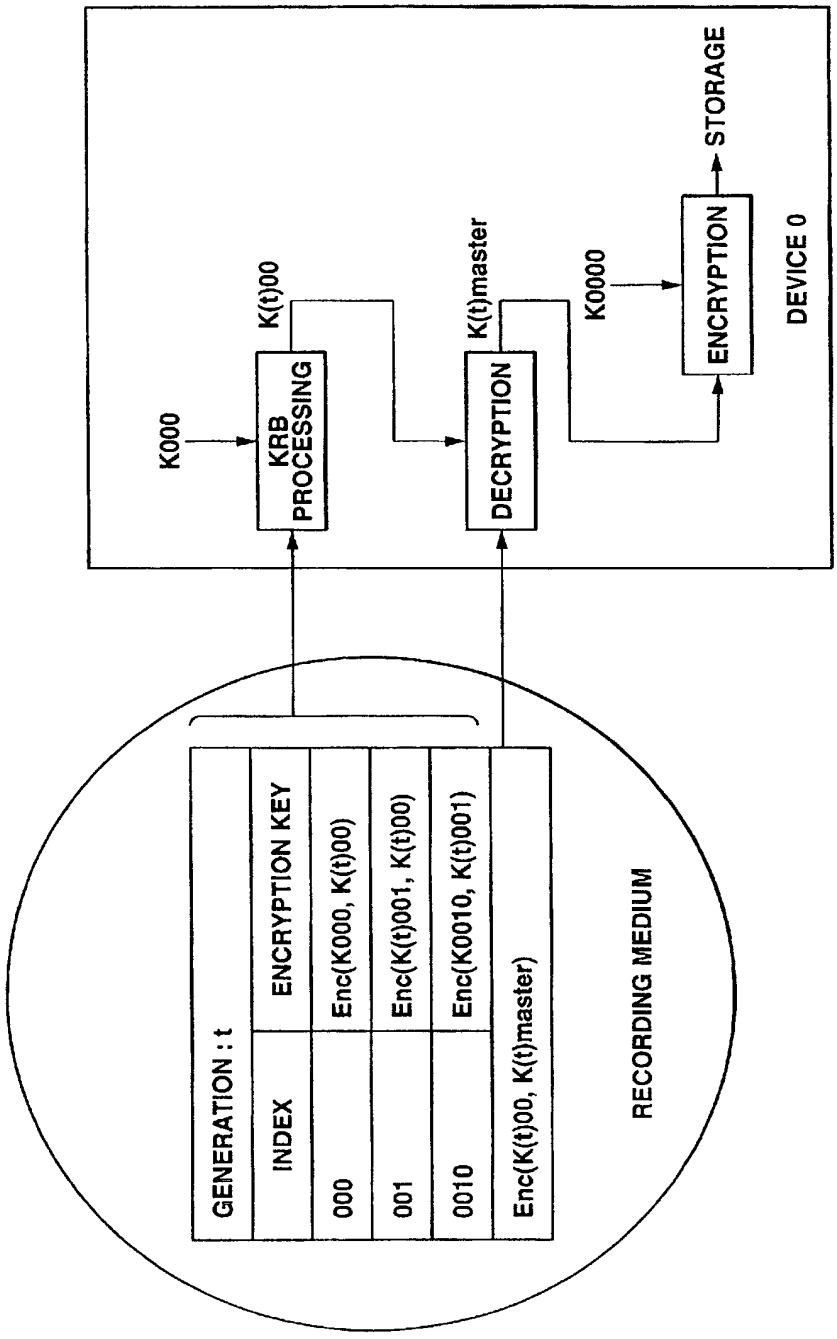

K000
KRB PROCESSING
K(t)00
DECRYPTION
K(t)master
K0000
ENCRYPTION
STORAGE
DEVICE 0
GENERATION : t
INDEX
ENCRYPTION KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
RECORDING MEDIUM

FIG.34

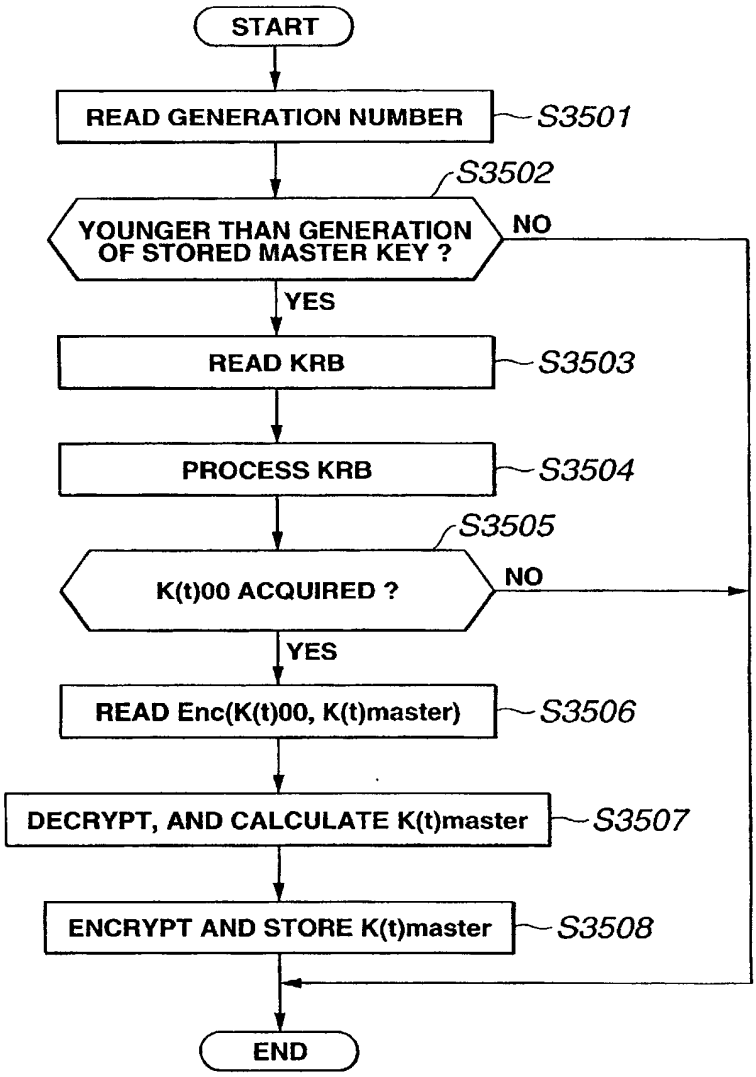

START
READ GENERATION NUMBER
S3501
S3502
YOUNGER THAN GENERATION OF STORED MASTER KEY ?
NO
YES
READ KRB
S3503
PROCESS KRB
S3504
S3505
K(t)00 ACQUIRED ?
NO
YES
READ Enc(K(t)00, K(t)master)
S3506
DECRYPT, AND CALCULATE K(t)master
S3507
ENCRYPT AND STORE K(t)master
S3508
END

FIG.35

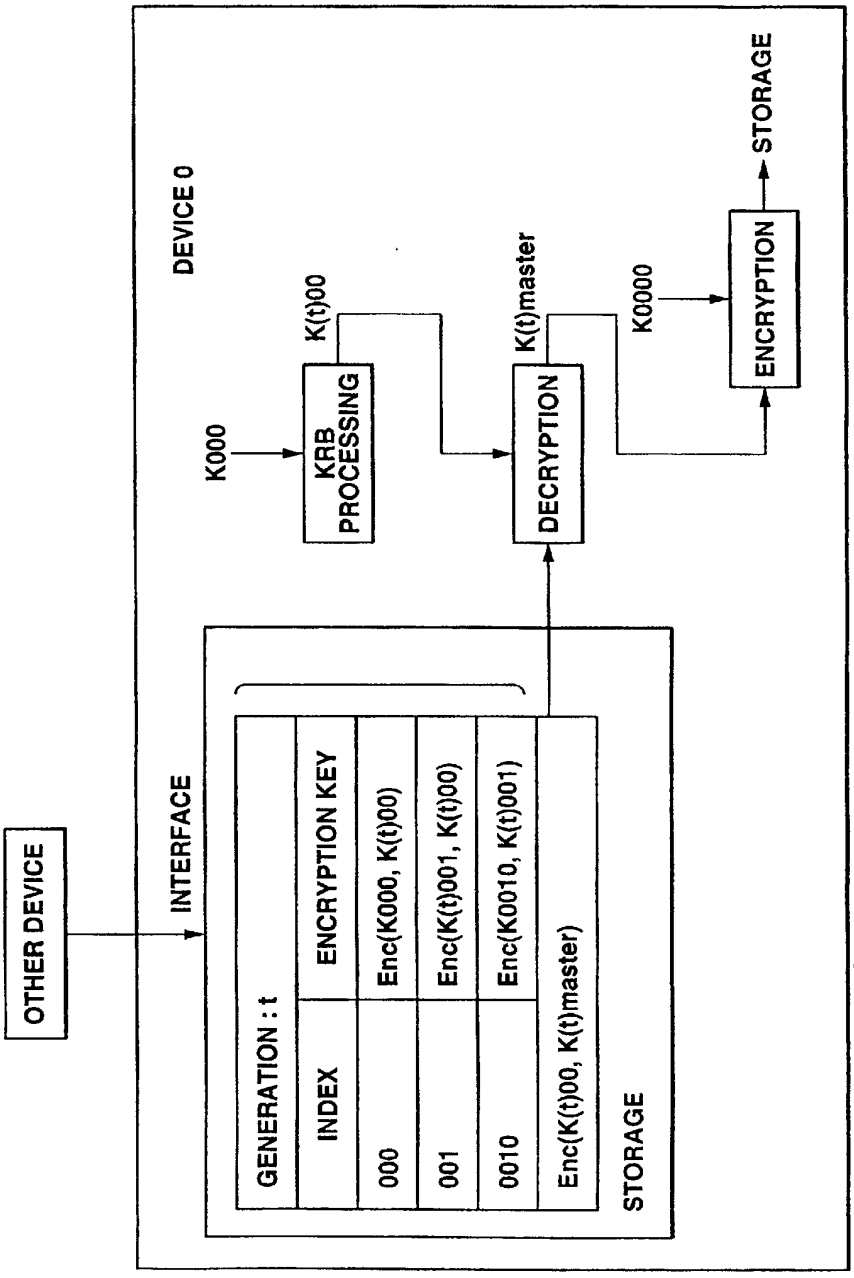

OTHER DEVICE
INTERFACE
DEVICE 0
K000
KRB PROCESSING
K(t)00
K(t)master
DECRYPTION
K0000
ENCRYPTION
STORAGE
GENERATION : t
INDEX
ENCRYPTION KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
STORAGE

FIG.36

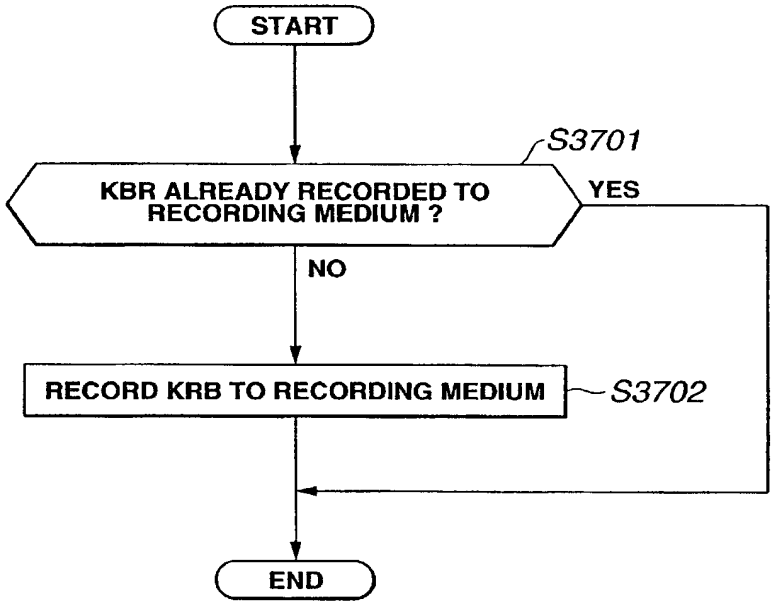

START
S3701
KBR ALREADY RECORDED TO RECORDING MEDIUM ?
YES
NO
RECORD KRB TO RECORDING MEDIUM
S3702
END

FIG.37

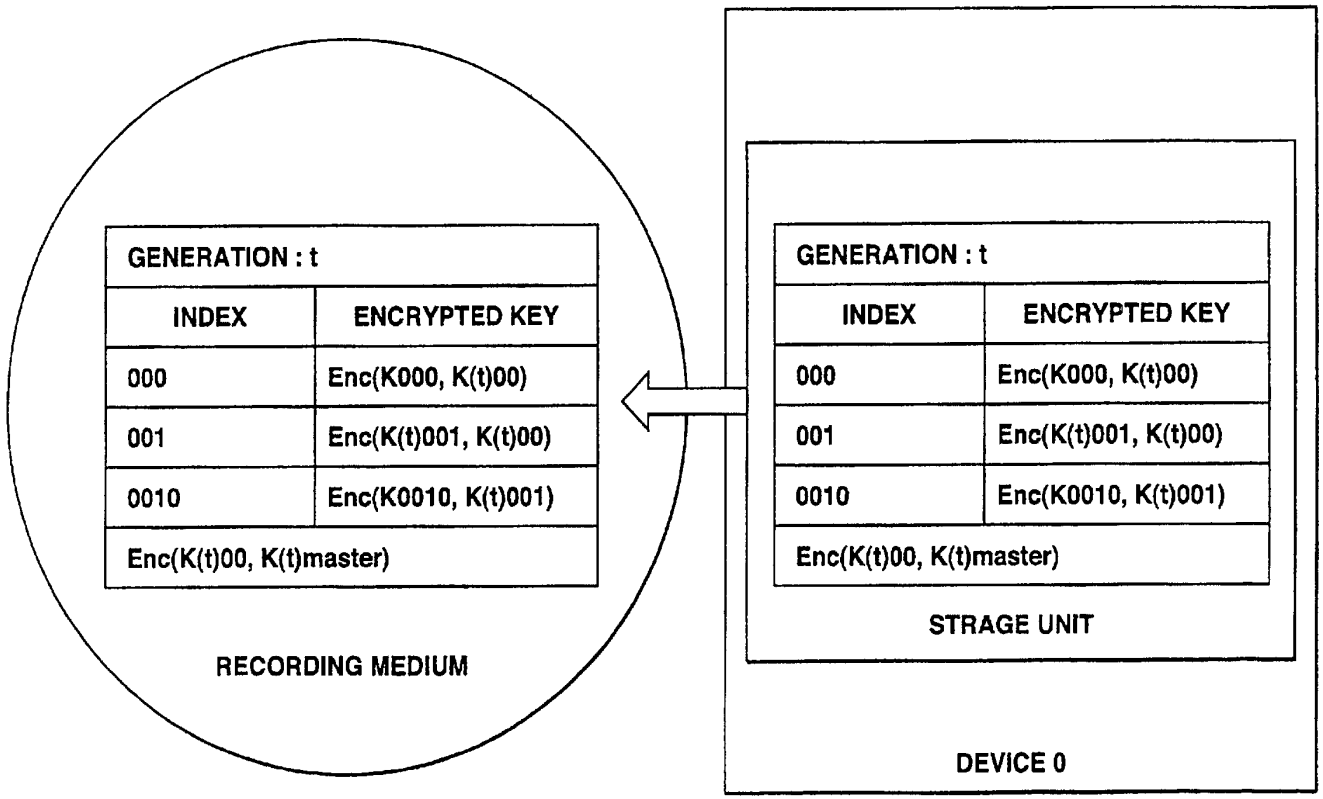

GENERATION : t
INDEX
ENCRYPTED KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
RECORDING MEDIUM
GENERATION : t
INDEX
ENCRYPTED KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
STRAGE UNIT
DEVICE 0

FIG.38

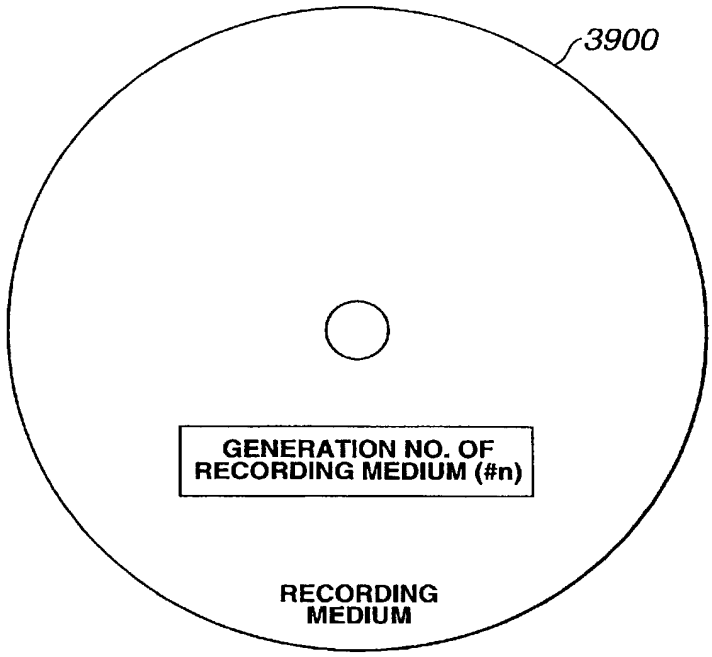


FIG.39

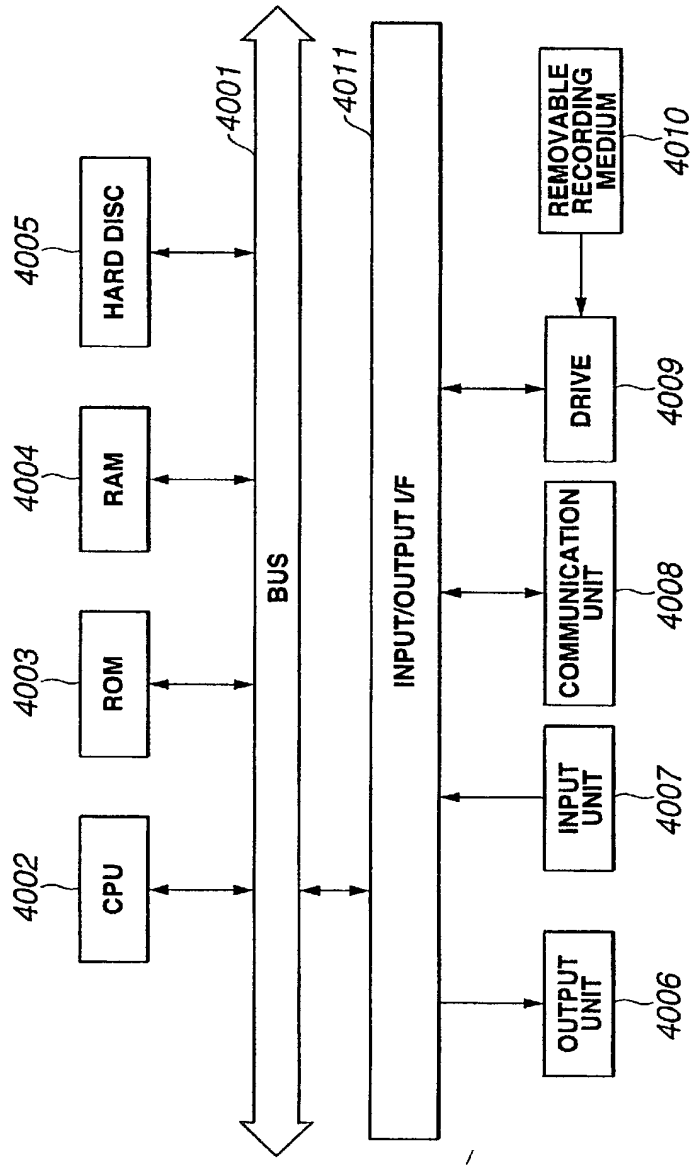

4001
BUS
4002
CPU
4003
ROM
4004
RAM
4005
HARD DISC
4006
OUTPUT UNIT
4007
INPUT UNIT
4008
COMMUNICATION UNIT
4009
DRIVE
4010
REMOVABLE RECORDING MEDIUM
4011
INPUT/OUTPUT I/F

FIG.40